Technical Disclosure Commons

Defensive Publications Series

October 2020

Hardware Security Key With Touch Pattern Recognition

Joseph Albert F. S. Pingenot

Hardware Security Key With Touch Pattern Recognition

ABSTRACT

A hardware security key for user authentication on computing devices is described. The security key is responsive to a user touch pattern and includes a set of conductive plates. Based on matching the entered pattern to a preset pattern, the security key transmits a secret to the computing device that enables the user to be authenticated. The pattern can include specific areas of the conductive plates that are touched in a particular sequence and/or a touch dwell time associated with the user touch. An LED can be provided on the security key to provide an indication to the user of a successful or unsuccessful authentication attempt.

KEYWORDS

- Security key
- Two-factor authentication (2FA)
- Cryptographic keys
- Conductive plate
- User authentication
- USB key

BACKGROUND

Hardware based security keys can be used in conjunction with passwords to provide additional security for online accounts, software applications, cloud storage, cloud applications, etc. Security information can be stored on a security key that attaches to a computer, e.g., via a USB port and is utilized to authenticate a user.

DESCRIPTION

This disclosure described a security key for user authentication on computing devices. The security key is responsive to a user touch pattern and includes a set of conductive plates that are provided on the security key. Based on a match of an entered pattern to a pattern previously set up by a user, the security key transmits a corresponding secret to the computing device. The secret is used to authenticate the user. The pattern includes specific areas of the conductive plates that are touched in a particular sequence and/or a touch dwell/absence time (duration of touch or lack thereof) associated with the user touch.

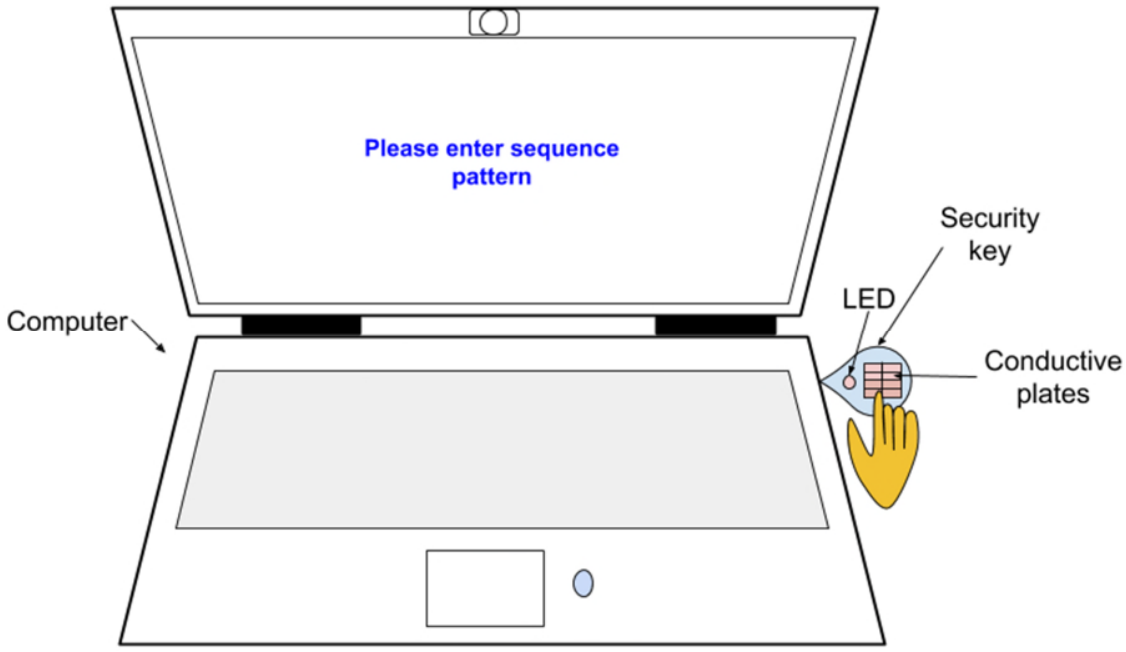

Fig. 1: A pattern is entered by touching conductive plates on a security key

Fig. 1 depicts an example of the use of a security key to authenticate a user, per techniques of this disclosure. In this illustrative example, the user is depicted utilizing their security key to obtain access to a software application on their computer.

The user connects their security key to the computer, e.g. by utilizing a USB port on the computer. When prompted, e.g., “please enter sequence pattern” as shown in Fig. 1, the user enters a preset pattern by touching conductive plates on the security key. The pattern includes touching particular plates on the security key in a specified sequence and/or with a specified touch dwell time.

Upon a match of the entered pattern with the preset pattern, the user is authenticated by the transmission of the secret from the security key to the computer. The user obtains access to the application. If the entered pattern does not match the preset pattern, the secret is not emitted, and an error is returned instead. An LED can be utilized to provide an indication to the user of a successful or unsuccessful authentication attempt.

Prior to use for authentication, a tap pattern is initially established by the user. When requested, the user touches the conductive plate (or multiple plates) in a pattern. A confirmation is provided to the user of the pattern being established. For example, the confirmation can be provided via a displayed dialog on a computer display and/or an LED light on the security key. The user can be requested to re-enter the pattern for confirmation.

CONCLUSION

A hardware security key for user authentication on computing devices is described. The security key is responsive to a user touch pattern and includes a set of conductive plates. Based on matching the entered pattern to a preset pattern, the security key transmits a secret to the computing device that enables the user to be authenticated. The pattern can include specific areas of the conductive plates that are touched in a particular sequence and/or a touch dwell time associated with the user touch. An LED can be provided on the security key to provide an indication to the user of a successful or unsuccessful authentication attempt.

REFERENCES

1. "How to Improve Your Online Security" available online at https://www.signalfox.org/2fa-security/ last accessed 29 September 2020.
2. https://onlykey.io/ last accessed 29 September 2020.
3. https://www.nitrokey.com/ last accessed 29 September 2020.